SUMMARY

DEPARTMENT OF DEFENSE CYBER STRATEGY

2018

This page left intentionally blank

INTRODUCTION

American prosperity, liberty, and security depend upon open and reliable access to information. The Internet empowers us and enriches our lives by providing ever-greater access to new knowledge, businesses, and services. Computers and network technologies underpin U.S. military warfighting superiority by enabling the Joint Force to gain the information advantage, strike at long distance, and exercise global command and control.

The arrival of the digital age has also created challenges for the Department of Defense (DoD) and the Nation. The open, transnational, and decentralized nature of the Internet that we seek to protect creates significant vulnerabilities. Competitors deterred from engaging the United States and our allies in an armed conflict are using cyberspace operations to steal our technology, disrupt our government and commerce, challenge our democratic processes, and threaten our critical infrastructure.

We are engaged in a long-term strategic competition with China and Russia. These States have expanded that competition to include persistent campaigns in and through cyberspace that pose long-term strategic risk to the Nation as well as to our allies and partners. China is eroding U.S. military overmatch and the Nation's economic vitality by persistently exfiltrating sensitive information from U.S. public and private sector institutions. Russia has used cyber-enabled information operations to influence our population and challenge our democratic processes. Other actors, such as North Korea and Iran, have similarly employed malicious cyber activities to harm U.S. citizens and threaten U.S. interests. Globally, the scope and pace of malicious cyber activity continue to rise. The United States' growing dependence on the cyberspace domain for nearly every essential civilian and military function makes this an urgent and unacceptable risk to the Nation.

The Department must take action in cyberspace during day-to-day competition to preserve U.S. military advantages and to defend U.S. interests. Our focus will be on the States that can pose strategic threats to U.S. prosperity and security, particularly China and Russia. We will conduct cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict. We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict. We will strengthen the security and resilience of networks and systems that contribute to current and future U.S. military advantages. We will collaborate with our interagency, industry, and international partners to advance our mutual interests.

During wartime, U.S. cyber forces will be prepared to operate alongside our air, land, sea, and space forces to target adversary weaknesses, offset adversary strengths, and amplify the effectiveness of other elements of the Joint Force. Adversary militaries are increasingly reliant on the same type of computer and network technologies that have become central to Joint Force warfighting. The Department will exploit this reliance to gain military advantage. The Joint Force will employ offensive cyber capabilities and innovative concepts that allow for the use of cyberspace operations across the full spectrum of conflict.

The *2018 Department of Defense Cyber Strategy* represents the Department's vision for addressing this threat and implementing the priorities of the *National Security Strategy* and *National Defense Strategy* for cyberspace. It supersedes the *2015 DoD Cyber Strategy*.

The United States cannot afford inaction: our values, economic competitiveness, and military edge are exposed to threats that grow more dangerous every day. We must assertively defend our interests in cyberspace below the level of armed conflict and ensure the readiness of our cyberspace operators to support the Joint Force in crisis and conflict. Our Soldiers, Sailors, Airmen, Marines, and civilian employees stand ready, and we will succeed.

STRATEGIC COMPETITION IN CYBERSPACE

The United States' strategic competitors are conducting cyber-enabled campaigns to erode U.S. military advantages, threaten our infrastructure, and reduce our economic prosperity. The Department must respond to these activities by exposing, disrupting, and degrading cyber activity threatening U.S. interests, strengthening the cybersecurity and resilience of key potential targets, and working closely with other departments and agencies, as well as with our allies and partners.

First, we must ensure the U.S. military's ability to fight and win wars in any domain, including cyberspace. This is a foundational requirement for U.S. national security and a key to ensuring that we deter aggression, including cyber attacks that constitute a use of force, against the United States, our allies, and our partners. The Department must defend its own networks, systems, and information from malicious cyber activity and be prepared to defend, when directed, those networks and systems operated by non-DoD Defense Critical Infrastructure (DCI)[1] and Defense Industrial Base (DIB)[2] entities. We will defend forward to halt or degrade cyberspace operations targeting the Department, and we will collaborate to strengthen the cybersecurity and resilience of DoD, DCI, and DIB networks and systems.

Second, the Department seeks to preempt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure that could cause a significant cyber incident regardless of whether that incident would impact DoD's warfighting readiness or capability. Our primary role in this homeland defense mission is to defend forward by leveraging our focus outward to stop threats before they reach their targets. The Department also provides public and private sector partners with indications and warning (I&W) of malicious cyber activity, in coordination with other Federal departments and agencies.

Third, the Department will work with U.S. allies and partners to strengthen cyber capacity, expand combined cyberspace operations, and increase bi-directional information sharing in order to advance our mutual interests.

The Department's cyberspace objectives are:

1. Ensuring the Joint Force can achieve its missions in a contested cyberspace environment;
2. Strengthening the Joint Force by conducting cyberspace operations that enhance U.S. military advantages;
3. Defending U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident;[3]
4. Securing DoD information and systems against malicious cyber activity, including DoD information on non-DoD-owned networks; and
5. Expanding DoD cyber cooperation with interagency, industry, and international partners.

DEFENDING CIVILIAN ASSETS THAT ENABLE U.S. MILITARY ADVANTAGE

The Department must be prepared to defend non-DoD-owned Defense Critical Infrastructure (DCI) and Defense Industrial Base (DIB) networks and systems. Our chief goal in maintaining an ability to defend DCI is to ensure the infrastructure's continued functionality and ability to support DoD objectives in a contested cyber environment. Our focus working with DIB entities is to protect sensitive DoD information whose loss, either individually or in aggregate, could result in an erosion of Joint Force military advantage. As the Sector Specific Agency (SSA) for the DIB and a business partner with the DIB and DCI, the Department will: set and enforce standards for cybersecurity, resilience, and reporting; and be prepared, when requested and authorized, to provide direct assistance, including on non-DoD networks, prior to, during, and after an incident.

[1] **"Defense Critical Infrastructure"** refers to the composite of DoD and non-DoD assets essential to project, support, and sustain military forces and operations worldwide (Department of Defense Directive 3020.40).

[2] **"Defense Industrial Base"** refers to the Department, Government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to satisfy military requirements (32 CFR Part 236).

[3] **"Significant cyber incident"** refers to an event occurring on or conducted through a computer network that is (or a group of related events that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people (Presidential Policy Directive 41).

STRATEGIC APPROACH

Our strategic approach is based on mutually reinforcing lines of effort to build a more lethal force; compete and deter in cyberspace; expand alliances and partnerships; reform the Department; and cultivate talent.

› BUILD A MORE LETHAL JOINT FORCE

Accelerate cyber capability development: The Department will accelerate the development of cyber capabilities for both warfighting and countering malicious cyber actors. Our focus will be on fielding capabilities that are scalable, adaptable, and diverse to provide maximum flexibility to Joint Force commanders. The Joint Force will be capable of employing cyberspace operations throughout the spectrum of conflict, from day-to-day operations to wartime, in order to advance U.S. interests.

Innovate to foster agility: The Department must innovate to keep pace with rapidly evolving threats and technologies in cyberspace. We will accept and manage operational and programmatic risk in a deliberate manner that moves from a "zero defect" culture to one that fosters agility and innovation because success in this domain requires the Department to innovate faster than our strategic competitors.

Leverage automation and data analysis to improve effectiveness: The Department will use cyber enterprise solutions to operate at machine speed and large-scale data analytics to identify malicious cyber activity across different networks and systems. The Department will leverage these advances to improve our own defensive posture and to ensure that our cyber capabilities will continue to be effective against competitors armed with cutting edge technology.

Employ commercial-off-the-shelf (COTS) cyber capabilities: The Department excels at creating cyber capabilities tailored for specific operational problems. In addition to these capabilities, we will make greater use of COTS capabilities that can be optimized for DoD use.

› COMPETE AND DETER IN CYBERSPACE

Deter malicious cyber activities: The United States seeks to use all instruments of national power to deter adversaries from conducting malicious cyberspace activity that would threaten U.S. national interests, our allies, or our partners. The Department will prioritize securing sensitive DoD information and deterring malicious cyber activities that constitute a use of force against the United States, our allies, or our partners. Should deterrence fail, the Joint Force stands ready to employ the full range of military capabilities in response.

Persistently contest malicious cyber activity in day-to-day competition: The Department will counter cyber campaigns threatening U.S. military advantage by defending forward to intercept and halt cyber threats and by strengthening the cybersecurity of systems and networks that support DoD missions. This includes working with the private sector and our foreign allies and partners to contest cyber activity that could threaten Joint Force missions and to counter the exfiltration of sensitive DoD information.

Increase the resilience of U.S. critical infrastructure: The Department will work with its interagency and private sector partners to reduce the risk that malicious cyber activity targeting U.S. critical infrastructure could have catastrophic or cascading consequences. We will streamline our public-private information-sharing mechanisms and strengthen the resilience and cybersecurity of critical infrastructure networks and systems.

› STRENGTHEN ALLIANCES AND ATTRACT NEW PARTNERSHIPS

Build trusted private sector partnerships: The private sector owns and operates the majority of U.S. infrastructure and is on the frontlines of nation-state competition in cyberspace. In coordination with other Federal departments and agencies, the Department will build trusted relationships with private sector entities that are critical enablers of military operations and carry out deliberate planning and collaborative training that enables mutually supporting cybersecurity activities.

Operationalize international partnerships: Many of the United States' allies and partners possess advanced cyber capabilities that complement our own. The Department will work to strengthen the capacity of these allies and partners and increase DoD's ability to leverage its partners' unique skills, resources, capabilities, and perspectives. Information-sharing relationships with allies and partners will increase the effectiveness of combined cyberspace operations and enhance our collective cybersecurity posture.

Reinforce norms of responsible State behavior in cyberspace: The Department will reinforce voluntary, non-binding norms of responsible State behavior in cyberspace during peacetime. The United States has endorsed the work done by the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) to develop a framework of responsible State behavior in cyberspace. The principles developed by the UNGGE include prohibitions against damaging civilian critical infrastructure during peacetime and against allowing national territory to be used for intentionally wrongful cyber activity. The Department will work alongside its interagency and international partners to promote international commitments regarding behavior in cyberspace as well as to develop and implement cyber confidence building measures (CBM). When cyber activities threaten U.S. interests, we will contest them and we will be prepared to act, in conjunction with partners, to defend U.S. interests.

› REFORM THE DEPARTMENT

Incorporate cyber awareness into DoD institutional culture: The Department will adapt its institutional culture so individuals at every level are knowledgeable about the cyberspace domain and can incorporate that knowledge into their day-to-day activities. Leaders and their staffs need to be "cyber fluent" so they can fully understand the cybersecurity implications of their decisions and are positioned to identify opportunities to leverage the cyberspace domain to gain strategic, operational, and tactical advantages.

Increase cybersecurity accountability: Reducing the Department's "attack surface" requires an increase in cybersecurity awareness and accountability across the Department. We will hold DoD personnel and our private sector partners accountable for their cybersecurity practices and choices.

Seek material solutions that are affordable, flexible, and robust: The Department will reduce the time it takes to procure software and hardware in order to keep pace with the rapid advance of technology. We will identify opportunities to procure scalable services, such as cloud storage and scalable computing power, to ensure that our systems keep pace with commercial information technology and can scale when necessary to match changing requirements. We will also leverage COTS capabilities where feasible to reduce our reliance on expensive, custom-built software that is difficult to maintain or upgrade.

Expand crowd-sourced vulnerability identification: The Department will continue to identify crowd-sourcing opportunities, such as hack-a-thons and bug-bounties, in order to identify and mitigate vulnerabilities more effectively and to foster innovation.

› CULTIVATE TALENT

Sustain a ready cyber workforce: The Department's workforce is a critical cyber asset. We will invest in building future talent, identifying and recruiting sought-after talent, and retaining our current cyber workforce. We will provide ample opportunities—both inside and outside the Department—for the professional development and career progression of cyber personnel. We will create processes for maintaining visibility of the entire military and civilian cyber workforce and optimizing personnel rotations across military departments and commands, including maximizing the use of the Reserve Components. The Department will also ensure that its cyber requirements are filled by the optimal mix of military service members, civilian employees, and contracted support to serve mission requirements.

Enhance the Nation's cyber talent: The Department plays an essential role in enhancing the Nation's pool of cyber talent in order to further the goal of increasing national resilience across the private and public sectors. To that end, we will increase our efforts alongside other Federal departments and agencies to promote science, technology, engineering, mathematics, and foreign language (STEM-L) disciplines at the primary and secondary education levels throughout the United States. The Department will also partner with industry and academia to establish standards in training, education, and awareness that will facilitate the growth of cyber talent in the United States.

Embed software and hardware expertise as a core DoD competency: To make it attractive to skilled candidates, the Department will establish a career track for computer science related specialties (including hardware engineers, software developers, and data analysts) that offers meaningful challenges, rotational billets at other Federal departments and agencies, specialized training opportunities tied to retention commitments, and the expansion of compensation incentives for the Cyber Excepted Service (CES).

Establish a cyber top talent management program: The Department will establish a cyber talent management program that provides its most skilled cyber personnel with focused resources and opportunities to develop key skills over the course of their careers. The Department will use competitive processes, including individual and team competitions, to identify the most capable DoD military and civilian cyber specialists and then empower those personnel to solve the Department's toughest challenges.

CONCLUSION

The arrival of the cyber era has created new opportunities and challenges for the Department and the Nation. Open and reliable access to information is a vital U.S. interest, and our allies and competitors alike should understand that we will assertively defend it. The *2018 DoD Cyber Strategy* directs the Department to defend forward, shape the day-to-day competition, and prepare for war by building a more lethal force, expanding alliances and partnerships, reforming the Department, and cultivating talent, while actively competing against and deterring our competitors. Taken together, these mutually reinforcing activities will enable the Department to compete, deter, and win in the cyberspace domain.

DEPARTMENT OF DEFENSE

UNITED STATES OF AMERICA